Field

Definition: A *field* is a set F together with two *commutative* binary operations $+$ and $\cdot$, where $(F, +)$ and $(F \setminus 0, \cdot)$ are (Abelian) groups, and moreover $\forall a, b, c \in F : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

In other words the following axioms have to be satisfied:

- $\forall a, b \in F : a + b = b + a$
- $\forall a, b, c \in F : (a + b) + c = a + (b + c)$
- $\exists 0 \in F \; \forall a \in F : a + 0 = a$
- $\forall a \in F \; \exists - a \in F : a + (-a) = 0$
- $\forall a, b \in F : a \cdot b = b \cdot a$ . . . including 0 !
- $\forall a, b, c \in F \setminus 0 : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $\exists 1 \in F \setminus 0 \; \forall a \in F \setminus 0 : a \cdot 1 = a$ . . . implies $1 \neq 0$
- $\forall a \in F \setminus 0 \; \exists a^{-1} \in F \setminus 0 : a \cdot a^{-1} = 1$
- $\forall a, b, c \in F : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

The product symbol $\cdot$ is often omitted and it has priority to $+$.

Examples

$(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$, briefly $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, are fields.

$\mathbb{Z}_p$ residue classes modulo a *prime* p are fields ($\mathbb{Z}_4$ and $\mathbb{Z}_6$ are not!)

$\mathbb{Z}_7$:

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

These binary operations $+$ and $\cdot$ satisfy all axioms.

In particular, the negative and inverse elements are:

x	0	1	2	3	4	5	6
$-x$	0	6	5	4	3	2	1

x	0	1	2	3	4	5	6
x^{-1}		1	4	5	2	3	6

The set $\left\{\frac{p(x)}{q(x)}\right\}$ with p, q polynomials with real coefficients forms the field $\mathbb{R}(x)$ of *real rational functions*.

Metatheorem

Metatheorem: All statements about systems of equations, matrices and calculations over $\mathbb{R}$ are valid also for any field F.

Metaproof: The proofs shown used from $\mathbb{R}$ only the field axioms.

Example: Solving a system $\boldsymbol{Ax} = \boldsymbol{b}$ over $\mathbb{Z}_7$:

Transform the augmented matrix into the echelon form:

$$\left(\begin{array}{cccc|c} 1 & 2 & 4 & 0 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 3 & 1 & 2 & 1 & 0 \end{array}\right) \underset{+4\,\mathrm{I}}{\sim} \left(\begin{array}{cccc|c} 1 & 2 & 4 & 0 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 0 & 2 & 4 & 1 & 4 \end{array}\right) \underset{+5\,\mathrm{II}}{\sim} \left(\begin{array}{cccc|c} 1 & 2 & 4 & 0 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) = (\boldsymbol{A}'|\boldsymbol{b}')$$

If the last column does not contain a pivot then solve $\boldsymbol{A}\bar{\boldsymbol{x}} = \boldsymbol{0}$:

$$\begin{array}{rcccccl} \bar{x}_2 & = & -4\bar{x}_4 - 2\bar{x}_3 & = & 3\bar{x}_4 + 5\bar{x}_3 & & \\ \bar{x}_1 & = & -4\bar{x}_3 - 2\bar{x}_2 & = & 3\bar{x}_3 + 5(3\bar{x}_4 + 5\bar{x}_3) & = & \bar{x}_4 \end{array}$$

Replace the free variables: $\bar{\boldsymbol{x}} = p_1(0,5,1,0)^\mathsf{T} + p_2(1,3,0,1)^\mathsf{T}$

Add some solution of $\boldsymbol{A}'\boldsymbol{x} = \boldsymbol{b}'$, e.g. $(4,2,0,0)^\mathsf{T}$ and get:

$$\boldsymbol{x} = (4,2,0,0)^\mathsf{T} + p_1(0,5,1,0)^\mathsf{T} + p_2(1,3,0,1)^\mathsf{T}$$

Metatheorem

Metatheorem: All statements about systems of equations, matrices and calculations over $\mathbb{R}$ are valid also for any field F.

Example: A matrix inversion over $\mathbb{Z}_5$:

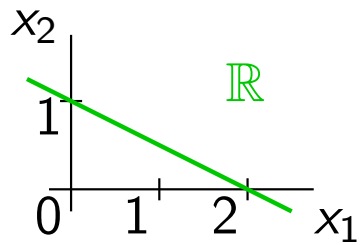
$$(\boldsymbol{A}|\mathbf{I}) = \left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 1 & 0 & 0 \\ 3 & 4 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \begin{matrix} \\ +2\,\mathrm{I} \\ \\ \end{matrix} \sim \left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 1 & 0 & 0 \\ 0 & 0 & 4 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \begin{matrix} +2\,\mathrm{III} \\ \mathrm{III} \sim \\ -\mathrm{II} \end{matrix}$$

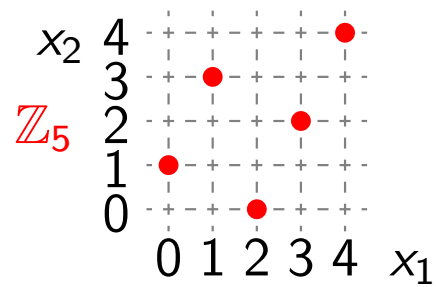
$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 4 & 1 & 0 & 2 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 3 & 4 & 0 \end{array}\right) \begin{matrix} +\mathrm{III} \\ -\mathrm{III} \sim \\ \\ \end{matrix} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 4 & 4 & 2 \\ 0 & 1 & 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 3 & 4 & 0 \end{array}\right) = (\mathbf{I}|\boldsymbol{A}^{-1})$$

Test:

$\boldsymbol{A}\boldsymbol{A}^{-1}=\mathbf{I}$			4	4	2
			2	1	1
			3	4	0
1	3	2	1	0	0
3	4	0	0	1	0
0	1	1	0	0	1

Warning: Geometric interpretation may differ!
In $\mathbb{R}$ the solutions of $x_1 + 2x_2 = 2$ form a line, while in $\mathbb{Z}_5$ this equation has only 5 solutions.





Field properties

Since $(F, +)$ and $(F \setminus 0, \cdot)$ are groups, we have already proved:

- uniqueness of elements 0 and 1, ... from the uniqueness of e,
- the uniqueness of $-a$, and the uniqueness of a^{-1} for $a \neq 0$,
- validity of eq. transforms: $c = d \Leftrightarrow ac + b = ad + b$ for $a \neq 0$,
- solubility of equations: $ax + b = c \Leftrightarrow x = \frac{c-b}{a}$ for $a \neq 0$.

Observation: For any $a \in F$ it holds that $0a = 0$ and $(-1)a = -a$.

Proof:

$$0a = 0a + 0 = 0a + (0a - 0a) = (0 + 0)a - 0a = 0a - 0a = 0$$

$$\begin{aligned}(-1)a &= (-1)a + 0 = (-1)a + a - a = (-1)a + 1a - a \\ &= (-1 + 1)a - a = 0a - a = 0 - a = -a\end{aligned}$$

Observation: If $ab = 0$ then $a = 0$ or $b = 0$.

Proof: By contradiction, if $a, b \neq 0$ then $\exists a^{-1}, b^{-1}$.
Then $1 = aa^{-1}bb^{-1} = aba^{-1}b^{-1} = 0a^{-1}b^{-1} = 0$ a contradiction.

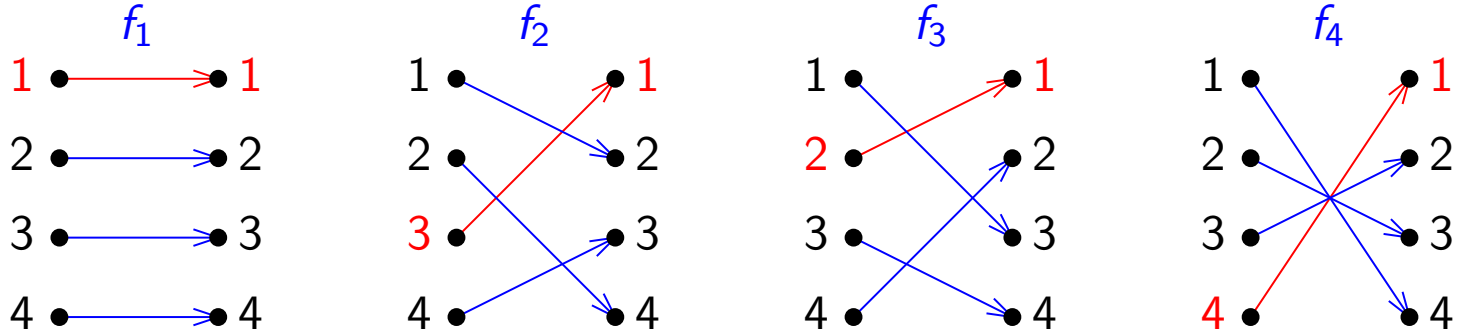
Fields from modular arithmetic

Theorem: $\mathbb{Z}_p$ is a field if and only if p is a prime.

Proof: $\Rightarrow$: If $p = ab$ was composed then $ab \equiv 0 \pmod{p}$,
a contradiction with the observation.

$\Leftarrow$: Most of the axioms follow from the properties of $+$ and $\cdot$ on $\mathbb{Z}$.
The only different is the existence of the inverse element a^{-1}:
$\forall a \in \{1, \ldots, p-1\}\ \exists a^{-1} \in \{1, \ldots, p-1\} : aa^{-1} \equiv 1 \pmod{p}$.

Define $f_a : \{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ by $f_a(x) = ax \mod p$.
The sought a^{-1} satisfies $f_a(a^{-1}) = 1$, i.e. it suffices to show that 1
belongs to the range of f_a. We prove indeed that f_a is surjective.



$f_1(1) = 1 \cdot 1 = 1$ $f_2(3) = 2 \cdot 3 = 1$ $f_3(2) = 3 \cdot 2 = 1$ $f_4(4) = 4 \cdot 4 = 1$

$1^{-1} = 1$ $2^{-1} = 3$ $3^{-1} = 2$ $4^{-1} = 4$

Fields from modular arithmetic

Theorem: $\mathbb{Z}_p$ is a field if and only if p is a prime.

Proof: $\Rightarrow$: If $p = ab$ was composed then $ab \equiv 0 \pmod{p}$,
a contradiction with the observation.

$\Leftarrow$: Most of the axioms follow from the properties of $+$ and $\cdot$ on $\mathbb{Z}$.
The only different is the existence of the inverse element a^{-1}:
$\forall a \in \{1, \ldots, p-1\}\ \exists a^{-1} \in \{1, \ldots, p-1\} : aa^{-1} \equiv 1 \pmod{p}$.

Define $f_a : \{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ by $f_a(x) = ax \mod p$.
The sought a^{-1} satisfies $f_a(a^{-1}) = 1$, i.e. it suffices to show that 1
belongs to the range of f_a. We prove indeed that f_a is surjective.

Since f_a maps a finite set onto itself, it is surjective if and only if it
is injective.

If f_a was not injective then $\exists b, c$ w.l.o.g. $b > c$ s.t.
$f_a(b) = f_a(c) \Rightarrow 0 = f_a(b) - f_a(c) \equiv ab - ac = a(b-c) \pmod{p}$,
in contrary with p being a prime as $a, b - c \in \{1, \ldots, p-1\}$.

Galois fields

Theorem: A field of size n exists if and only if n is a power of prime. It is unique upto isomorphism. We denote it by $GF(n)$.

Example: The field $GF(4) = GF(2^2)$: For $F = \{0, 1, a, b\}$ define the addition and multiplication as:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

These operations $+$ and $\cdot$ satisfy all axioms.

Another view on the same field: take F as all polynomials of the maximum degree 1 with coefficients in $\mathbb{Z}_2$, e.g. $a = x$, $b = x + 1$. The multiplication is done modulo the polynomial $x^2 + x + 1$.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Characteristic

Definition: For a field F, if for some $n \in \mathbb{N}$: $\underbrace{1+1+\cdots+1}_{n\times} = 0$

then the smallest such n is the *characteristic* of the field F.
Otherwise the field F has characteristic 0. It is denoted $\mathrm{char}(F)$.

Example: $\mathrm{char}(\mathbb{R}) = 0$ and $\mathrm{char}(\mathbb{Z}_p) = p$.

Theorem: The field characteristic is always a prime or 0.

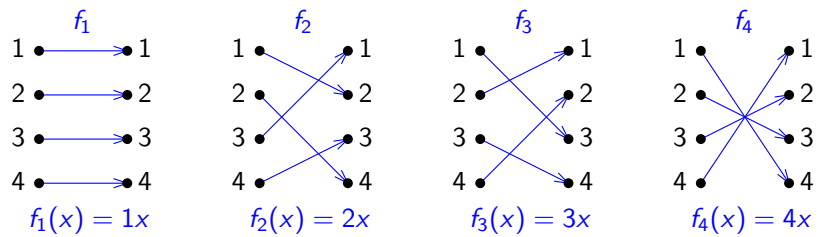
Proof: By contrary, if the characteristic was composed $n = ab$, then
$0 = \underbrace{1+1+\cdots+1}_{n\times} = \underbrace{(1+1+\cdots+1)}_{a\times}\underbrace{(1+1+\cdots+1)}_{b\times} \neq 0$
as both $\underbrace{1+1+\cdots+1}_{a\times} \neq 0$ and $\underbrace{1+1+\cdots+1}_{b\times} \neq 0$.

Observation: In fields of characteristic 2 each element is self-inverse and subtraction can be replaced by addition.
Proof: $1+1=0 \;\Rightarrow\; -1=1 \;\Rightarrow\; -a=a \;\Rightarrow\; a-b=a+b$.

Fermat's little theorem

Theorem: [Fermat 1640•, Leibnitz 1683+, Euler 1736*]
For any prime p and any $a \in \{1, \ldots, p-1\}$: $a^{p-1} \equiv 1 \pmod{p}$.

Proof: The map $f_a : x \to ax$ is in $\mathbb{Z}_p$ a bijection on $\{1, \ldots, p-1\}$.



Thus in $\mathbb{Z}_p$ we get

$$\prod_{x=1}^{p-1} x = \prod_{x=1}^{p-1} f_a(x) = \prod_{x=1}^{p-1} ax = a^{p-1} \prod_{x=1}^{p-1} x$$

and after cancelling $\prod_{x=1}^{p-1} x$ also $1 = a^{p-1}$.

Corollary: In $\mathbb{Z}_p$ with p prime any a satisfies $a^p = a$.
Non-zero a has inverse $a^{-1} = a^{p-2}$.

Pierre de Fermat
1607 – 1665
Pict. Wikipedia

•w/o proof, +unpublished, *published

Questions to understand the lecture topic

- Is there any structure $(S, +, \cdot)$ satisfying the distributive axiom, where $(S, +)$ and $(S, \cdot)$ are groups with the same neutral element?
- Which axioms from the definition of a field were used in the proofs of the following statements:
  - Adding the i-th row to the j-th row is an equivalent row transformation.
  - Every solution of a system of linear equations can be obtained by backward substitution.
  - The rank of a matrix is defined uniquely.
  - Matrix multiplication is associative.
  - $\boldsymbol{A}^{-1}\boldsymbol{A} = \mathbf{I}$.

  Which axioms were not needed in these proofs?
- Does the relation $a^m \cdot a^n = a^{m+n}$ hold in fields? If so, for what possible exponents m and n?
- Let us have a square matrix $\boldsymbol{A}$ with elements from the set $\{0, 1, 2\}$. How can the regularity of $\boldsymbol{A}$ change if we interpret its content over different fields, such as $\mathbb{R}, \mathbb{Q}, \mathbb{Z}_3, \mathbb{Z}_5$, etc.?